PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-073309
(43)Date of publication of application : 16.03.1999

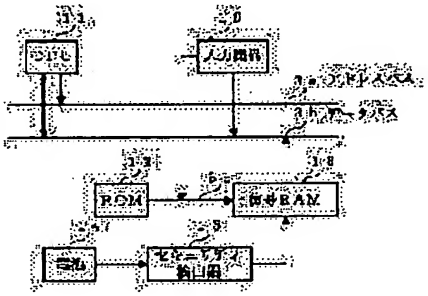
(51)Int.Cl. G06F 9/06

(21)Application number : 09-231381
(22)Date of filing : 27.08.1997

(71)Applicant : NEC CORP
(72)Inventor : WATANABE TAKASHI

(54) INSTRUCTION CODE PROTECTION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To attain a simple instruction code protection system capable of preventing an instruction code stored in an ROM from being easily analyzed.
SOLUTION: A CPU 11 outputs the address of an instruction code or data to be accessed to an address bus 3a and an ROM 12 stores a ciphered instruction code outputted from the CPU 11. A decoding RAM 13 inputs the ciphered instruction code outputted from the ROM 12 as an address and stores conversion data to be decoded and a decoded instruction code is sent to the CPU 11 through a data bus 3b. A battery 14 supplies power for storing the conversion data stored in the RAM 13. A security detector 15 detects action intending the analysis of the instruction code and stops power supply from the battery 14 to the RAM 13. An input mechanism 16 writes the contents of the RAM 13 from the external independently of the operation of the CPU 11.



LEGAL STATUS

[Date of request for examination]	27.08.1997
[Date of sending the examiner's decision of rejection]	10.07.2001
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	
[Date of registration]	
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－73309

(43)公開日　平成11年(1999)３月16日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　9/06	５５０	Ｇ０６Ｆ　9/06	５５０Ｂ

審査請求　有　　請求項の数４　ＯＬ　（全４頁）

(21)出願番号　特願平9－231381

(22)出願日　平成９年(1997)８月27日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　渡邊　貴志
東京都港区芝五丁目７番１号　日本電気株式会社内

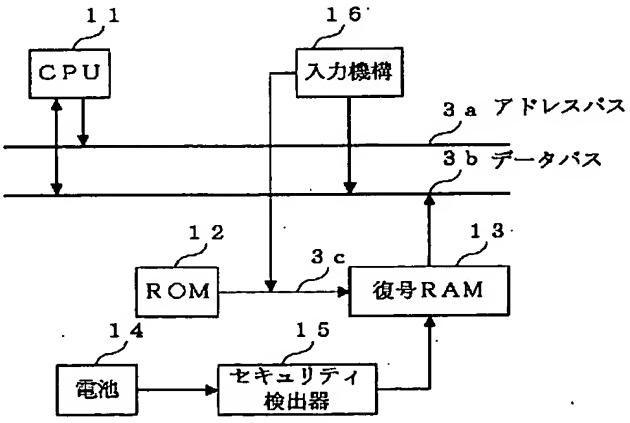
(74)代理人　弁理士　京本　直樹　（外２名）

(54)【発明の名称】　命令コード保護システム

(57)【要約】

【課題】　ＲＯＭに格納されている命令コードを容易に解析されないための簡便な命令コード保護システムを実現する。

【解決手段】　ＣＰＵ１１は、アドレスバス３ａにアクセスすべき命令コードやデータのアドレスを出力し、ＲＯＭ１２は暗号化されたＣＰＵ１１の命令コードを格納する。復号ＲＡＭ１３はＲＯＭ１２の出力した暗号化された命令コードをアドレス入力とし、復号化するための変換データを記憶し、復号された命令コードはデータバス３ｂを通してＣＰＵ１１へ送出される。電池１４は復号ＲＡＭ１３に記憶されている変換データを保持するための電力を供給する。セキュリティ検出器１５は命令コードの解析を意図した行為を検出して電池１４から復号ＲＡＭ１３への電力供給を停止する。入力機構１６はＣＰＵ１１の動作に無関係に復号ＲＡＭ１３の内容を外部から書き込む。



【特許請求の範囲】
【請求項１】（ａ）暗号化された命令コードを格納するリードオンリーメモリと、（ｂ）前記リードオンリーメモリからの暗号化された命令コードを復号しデータバスに出力するための変換データを記憶する揮発性の復号ランダムアクセスメモリと、（ｃ）前記復号ランダムアクセスメモリの記憶内容を保持するための電力を供給する電池と、（ｄ）命令コードの解析を意図した筐体の分解を含む操作を検出し前記電池から前記復号ランダムアクセスメモリに供給される電力を切断するセキュリティ検出器と、（ｅ）前記復号ランダムアクセスメモリに記憶される変換データを外部より書き込むための入力機構と、を備えることを特徴とする命令コード保護システム。
【請求項２】　前記リードオンリーメモリに対し、アドレスバスを介してアドレスを与え、前記復号ランダムアクセスメモリからの復号された命令コードを前記データバスを介して取り込むＣＰＵを備えることを特徴とする請求項１記載の命令コード保護システム。
【請求項３】　前記入力機構が、前記復号ランダムアクセスメモリに対し前記アドレスバスを介してアドレスを与え、前記データバスを介して前記変換データを書き込むことを特徴とする請求項２記載の命令コード保護システム。
【請求項４】　前記リードオンリーメモリおよび前記復号ランダムアクセスメモリを１チップで構成することを特徴とする請求項１、２または３記載の命令コード保護システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、保護システムに関し、特に、コンピュータのプログラムに使用される命令コードを解析から保護するための命令コードシステムに関する。
【０００２】
【従来の技術】従来の技術としては、たとえば、「特開平２－１５５０３４号公報」記載の「セキュリティ機能付き計算機」がある。この技術は、記憶装置上の機械語命令およびデータを中央処理装置に取り込んで解釈しながら実行する計算機であって、前記中央処理装置内に設けられる鍵格納用の格納手段と、この格納手段に格納されている鍵を用いて前記記憶装置から暗号化された機械語命令およびデータを読み出して中央処理装置で使用可能な機械語命令およびデータに復元する暗号復元手段と、前記格納手段に格納されている鍵を用いて前記記憶装置に格納されるデータを暗号化して前記記憶装置に格納する暗号化手段とを備える計算機である。
【０００３】
【発明が解決しようとする課題】上述した従来の技術の問題点は、暗号化・復号部と記憶装置とを別々に解析しても命令コードやデータの秘匿性は保たれるが、暗号化・復号部と記憶装置とを総合して解析すると、記憶装置内の命令コードやデータを解読することができ、セキュリティーが保証されないことである。その理由は、暗号化・復号部を中央処理装置内に持つからである。
【０００４】本発明の目的は、装置全体を解析しても、命令コードの秘匿性が維持がされセキュリティーが保証される命令コード保護システムを実現することである。
【０００５】
【課題を解決するための手段】本発明の第１の命令コード保護システムは、（ａ）暗号化された命令コードを格納するリードオンリーメモリと、（ｂ）前記リードオンリーメモリからの暗号化された命令コードを復号しデータバスに出力するための変換データを記憶する揮発性の復号ランダムアクセスメモリと、（ｃ）前記復号ランダムアクセスメモリの記憶内容を保持するための電力を供給する電池と、（ｄ）命令コードの解析を意図した筐体の分解を含む操作を検出し前記電池から前記復号ランダムアクセスメモリに供給される電力を切断するセキュリティ検出器と、（ｅ）前記復号ランダムアクセスメモリに記憶される変換データを外部より書き込むための入力機構と、を備える。
【０００６】本発明の第２の命令コード保護システムは、前記第１の命令コード保護システムであって、前記前記リードオンリーメモリに対し、アドレスバスを介してアドレスを与え、前記復号ランダムアクセスメモリからの復号された命令コードを前記データバスを介して取り込むＣＰＵを備える。
【００００７】本発明の第３の命令コード保護システムは、前記第２の命令コード保護システムであって、前記入力機構が、前記復号ランダムアクセスメモリに対し前記アドレスバスを介してアドレスを与え、前記データバスを介して前記変換データを書き込む。
【００００８】本発明の第４の命令コード保護システムは、前記第１、２または３の命令コード保護システムであって、前記リードオンリーメモリおよび前記復号ランダムアクセスメモリを１チップで構成する。
【００００９】
【発明の実施の形態】次に、本発明の実施の形態について図１を参照して詳細に説明する。図１は、本発明の実施の形態を示すブロック図である。
【００１０】図１を参照すると、本発明の命令コード保護システムは、アドレスバス３ａにアクセスすべき命令コードやデータのアドレスを出力し、データバス３ｂを用い命令コードやデータの入出力を行うＣＰＵ１１と、暗号化されたＣＰＵ１１の命令コードを格納するリードオンリーメモリであるＲＯＭ１２と、ＲＯＭ１２の出力した暗号化された命令コードをアドレス入力とし、復号化するための変換データを記憶し、復号された命令コードをデータバス３ｂを通してＣＰＵ１１へ送出するラン

ダムアクセスメモリである復号ＲＡＭ１３と、復号ＲＡＭ１３に記憶されている変換データを保持するための電力を供給する電池１４と、命令コードの解析を意図した筐体の分解等の行為を検出して電池１４から復号ＲＡＭ１３への電力供給を停止する機能を持つセキュリティ検出器１５と、ＣＰＵ１１の動作に無関係に復号ＲＡＭ１３の内容を外部から書き込むための入力機構１６とから構成される。

【００１１】次に、上記本発明の命令コード保護システムの動作に関して図１を参照して説明する。ＣＰＵ１１は命令コードを読み出す際にアドレスバス３ａにアクセスするアドレスを出力する。このアドレスは命令コードが暗号化されて格納されているＲＯＭ１２に与えられ、暗号化された命令コードがデータ線３ｃに出力される。

【００１２】暗号化された命令コードはデータ線３ｃ経由で復号ＲＡＭ１３へアドレスとして供給される。復号ＲＡＭ１３には暗号化されたアドレスパターンからデータを復号するための復号データがあらかじめ格納されている。データ線３ｃによって供給された暗号化された命令コードは復号ＲＡＭ１３の復号データによって復号化されデータバス３ｂ経由でＣＰＵ１１に供給される。以上の手順でＣＰＵ１１は正しい命令コードを得ることができる。

【００１３】復号ＲＡＭ１３内の復号データは電池１４の電力によって保持されているが、セキュリティ検出器１５が命令コードの解析を意図した筐体の分解等の行為を検出した場合には、電池１４から復号ＲＡＭ１３への電力供給が停止され、これにともない復号ＲＡＭ１３内の復号データは破壊される。以後、復号ＲＡＭ１３は復号機能を失い、またＲＯＭ１２は暗号化されているため命令コードを容易に解析することができない状態となる。

【００１４】また、入力機構１６を用いて復号ＲＡＭ１３へ復号データを書き込むことができる。

【００１５】次に本発明の実施の形態の実施例に関して図２を参照して詳細に説明する。図２は本発明の実施例を示すブロック図である。語長８ビットのＣＰＵ２１は、アドレスバス３ａにアクセスすべき命令コードやデータのアドレスを出力し、８ビットデータバス３ｂを用い命令コードやデータの入出力を行う。

【００１６】ＲＯＭ２２はデータビット位置を組み替えて暗号化されたＣＰＵ２１の命令コードを格納している。

【００１７】復号ＲＡＭ２３はＲＯＭ２２の出力した暗号化された命令コードをアドレス入力とし、正しいデータビット位置に組み替えて復号化するための変換データを記憶している。また、復号された命令コードは８ビットデータバス３ｂを通してＣＰＵ２１へ伝達される。復号ＲＡＭ２３は、「２の８乗」＝２５６［バイト］の容量を有すればよい。

【００１８】電池２４は復号ＲＡＭ２３に記憶されている変換データを保持するための電力を供給する。

【００１９】筐体分解検出センサ２５は命令コードの解析を意図した筐体の分解を検出するセンサ機能を有し、筐体の分解を検出した場合に電池２４から復号ＲＡＭ２３への電力供給を停止する機能を持つ。

【００２０】入力機構２６はＣＰＵ２１の動作に無関係に復号ＲＡＭ２３の内容を外部から書き込むための機構である。

【００２１】次に上記本発明の実施例の動作について図２を参照して説明する。ＣＰＵ２１は命令コードを読み出す際にアドレスバス３ａにアクセスするアドレスを出力する。このアドレスは命令コードが暗号化されて格納されているＲＯＭ２２に与えられ、暗号化された命令コードがデータ線３ｃに出力される。

【００２２】暗号化された命令コードはデータ線３ｃ経由で復号ＲＡＭ２３へアドレスとして供給される。復号ＲＡＭ２３には供給された暗号化されたアドレスパターンからデータを復号するための復号データがあらかじめ入力機構２６を用いて格納されている。データ線３ｃによって供給された暗号化された命令コードは復号ＲＡＭ２３の復号データによって復号化されデータバス３ｂ経由でＣＰＵ２１に供給される。以上の手順でＣＰＵ２１は正しい命令コードを得ることができる。

【００２３】復号ＲＡＭ２３内の復号データは電池２４の電力によって保持されているが、筐体分解検出センサ２５が命令コードの解析を意図した筐体の分解を検出した場合には、電池２４から復号ＲＡＭ２３への電力供給が停止され、これにともない復号ＲＡＭ２３内の復号データは破壊される。以後、復号ＲＡＭ２３は復号機能を失い、またＲＯＭ２２は暗号化されているため命令コードを容易に解析すするとができない状態となる。また、入力機構２６を用いて復号ＲＡＭ２３へ復号データを書き込むことができる。

【００２４】次に、筐体分解検出センサ２５の機能の詳細について図３を参照して説明する。図３は、筐体分解検出センサ２５の機能を示すブロック図である。筐体３１は、１面が開口した立方体あるいは直方体であり、その開口面は側板３２とネジ３４により密閉される。筐体分解検出センサ２５（マイクロスイッチ）は、筐体３１内に実装され、開口面に向かって接触感知センサ３３が突起している。また、信号線４ａは、電池２４に接続され、信号線４ｂは、複合ＲＡＭ２３に接続されている。

【００２５】側板３２が、ネジ３４により筐体３１に固定された状態では、接触感知センサ３３により信号線４ａと信号線４ｂとが接続された状態になり、電池２４から複合ＲＡＭ２３に電源が供給される。筐体を分解するために、ネジ３４をゆるめると、接触感知センサ３３により信号線４ａと信号線４ｂとが断続された状態になり、電池２４からの電源は、複合ＲＡＭ２３に供給され

なくなり、複合ＲＡＭ２３の内容は破壊される。

【００２６】また、ＲＯＭ２２および復号ＲＡＭ２３を１チップで構成し、実装効率を向上させることができる。

【００２７】

【発明の効果】本発明の第１の効果は、装置全体を解析しても、命令コードの秘匿性が維持がされセキュリティーが保証される命令コード保護システムを実現できることである。その理由は、復号手段を容易に復号手段を破壊することができる揮発性の復号ＲＡＭに格納し、命令コード自体は暗号化してＲＯＭに格納することにより、ＲＯＭを単独で解析しても容易に復号された命令コードを読み取ることができず、命令コードが保護されるからである。

【００２８】第２の効果は、実装効率を向上させることが可能となることである。その理由は、ＲＯＭおよび復号ＲＡＭを１チップで構成するからである。

【図面の簡単な説明】

【図１】本発明の実施の形態を示すブロック図である。

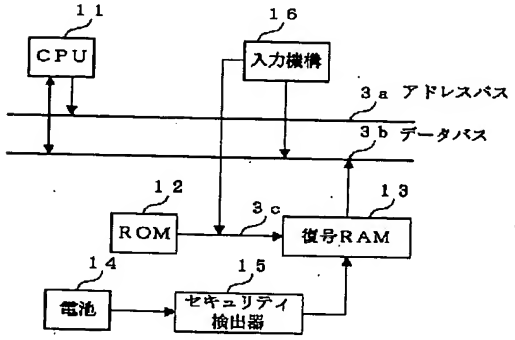
【図２】本発明の実施例を示すブロック図である。

【図３】図２の筐体分解検出センサの機能を示すブロック図である。

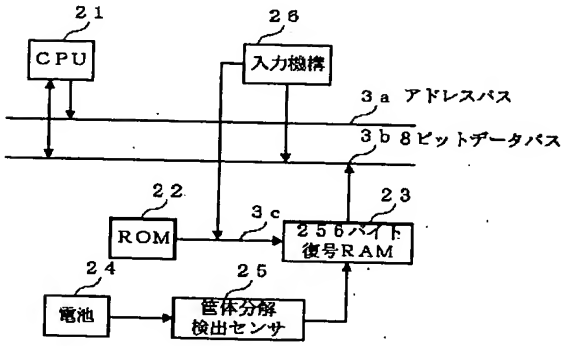
【符号の説明】

１１、２１　ＣＰＵ
１２、２２　ＲＯＭ
１３、２３　復号ＲＡＭ
１４、２４　電池
１５　セキュリティ検出器
１６、２６　入力機構
２５　筐体分解検出センサ
３ａ　アドレスバス
３ｂ　データバス
３ｃ　データ線
３１　筐体
３２　側板
３３　接触感知センサ
３４　ネジ
４ａ、４ｂ　信号線

【図１】



【図２】



【図３】